(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 May 2001 (17.05.2001)

PCT

(10) International Publication Number
WO 01/35193 A1

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/GB00/04266

(22) International Filing Date:
8 November 2000 (08.11.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/435,899 8 November 1999 (08.11.1999) US

(71) Applicant: INTERNATIONAL BUSINESS MACHINES CORPORATION [US/US]; New Orchard Road, Armonk, New York, NY 10504 (US).

(71) Applicant *(for MC only)*: IBM UNITED KINGDOM LIMITED [GB/GB]; P.O. Box 41, North Harbour, Portsmouth, Hampshire PO6 3AU (GB).

(72) Inventor: SEGER, Paul, Joseph; 5145 W. Paseo Del Barranco, Tucson, AZ 85745 (US).

(74) Agent: JENNINGS, Michael, John; IBM United Kingdom Limited, Intellectual Property Law, Hursley Park, Winchester, Hampshire SO21 2JN (GB).

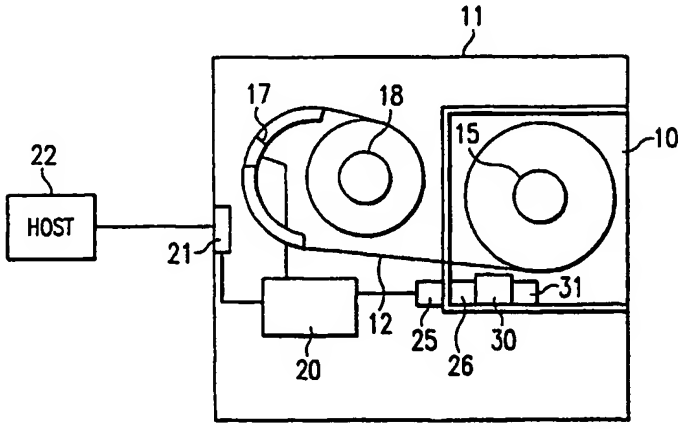
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: WIRELESS SECURITY ACCESS MANAGEMENT FOR A PORTABLE DATA STORAGE CARTRIDGE



(57) Abstract: A portable security system mounted in a portable data storage cartridge (10) for managing access by users to the cartridge (10). A programmable computer processor (30) mounted in the cartridge (10) is powered by and receives data from and transmits data to a data storage drive (11) via a wireless RF interface (26), when mounted in the drive. A user table has a unique user identifier for each authorized user and lists permitted activities the user is authorized to conduct with respect to the data storage cartridge (10). Preferably, a private key, public key algorithm is employed. Thus, the user identifier comprises a user symbol and a user decrypting sender public key. A user authentication message from the authorized user is encrypted by a sender private key and a receiver public key, in accordance with a predetermined algorithm, employing the cryptographic algorithm. The cryptographic algorithm decrypts the user authentication message employing a receiver private key and the sender public key, whereby the user authentication message is known to have come from the user. Then, the security system algorithm grants access to the user for the listed activities with respect to the cartridge (10).

WO 01/35193 A1

WIRELESS SECURITY ACCESS MANAGEMENT FOR A PORTABLE DATA STORAGE CARTRIDGE

FIELD OF THE INVENTION

This invention relates to the protection of data stored in portable data storage cartridges, and, more particularly, to providing secure access to the data stored in portable data storage cartridges.

BACKGROUND OF THE INVENTION

Data storage cartridges are typically employed to store data which may be transported between data storage drives and may be stored separately from the data storage drives between uses. Much of the data must be secured with respect to outsiders, and much of the data must be secured in favor of some users with respect to other users. Only certain users should be allowed access to certain data, and certain users should be allowed to define who has access to that data. An example comprises payroll information, and another example comprises financial account information. Further, the authorized users tend to change over time.

Thus, it is advantageous to not only provide security for data stored in data storage cartridges, but also to manage the access to that data to particular users, and to different users for different data storage cartridges.

Security of data stored in portable data storage cartridges is typically managed by encrypting the data and providing a key for decrypting the data. Typically, a data processing system includes or obtains the decryption key, and users which are authorized access to the data are listed in the data processing system. The data processing system provides the key and decrypts the data of the data storage drive accessing the data storage cartridge. One example is described in U.S. Patent No. 5,857,021 in which permission data is written into the data storage media of the cartridge which contains an encrypted key that is necessary for decrypting the data. The key can be decoded only with valid IDs of the equipment of the data processing system. The data processing system thus provides the decrypting key and the user is authorized access by a table in the data processing system.

A difficulty is that the access by a user to the data is not portable even though the data storage cartridge is portable. The access by a user is limited to a data processing system having the authorization table and having the decryption key.

Data processing systems are continually being updated and the authorization tables must be transferred to the new system, and correlated with the data storage media to which access is required. The management of the authorization table is typically handled by other organizations, such as IS, than those responsible for the security of the data. The changes to the table and correlation to the data and to the various data processing systems become a source of loss of security.

SUMMARY OF THE INVENTION

The present invention provides a security system which is portable and may be managed to accommodate changes to access to the data.

The present invention provides a portable security system, method, and computer readable program code of a computer program product, which resides in a portable data storage cartridge for managing access to the portable data storage cartridge. The data storage cartridge has a data storage media, such as a magnetic tape or an optical disk, for storing data for read/write access by a user of a data storage drive when mounted in the data storage drive.

The portable security system comprises a wireless interface mounted in the portable data storage cartridge for receiving power and data from, and sending data to, the data storage drive when mounted in the data storage drive. The wireless interface preferably comprises an RF interface. A programmable computer processor is mounted in the portable data storage cartridge and coupled to the wireless interface. The computer processor within the portable data storage cartridge is powered by the wireless interface and receives and transmits data to the data storage drive via the wireless interface. The computer processor provides a user table comprising at least one unique user identifier for each authorized user, which may comprise a user symbol and a corresponding user key, and at least one permitted activity the user is authorized to conduct with respect to the data storage media. The user identifier, when combined with a user authentication message from the authorized user in

accordance with a predetermined algorithm, authorizes the user. The computer processor within the portable data storage cartridge receives user authentication messages from the data storage drive via the wireless interface, and combines the user authentication message with the user identifier from the user table in accordance with the predetermined algorithm to authorize or deny the user activity, and transmits the user authorization or denial to the data storage drive via the wireless interface.

Preferably, a private key, public key cryptographic algorithm is employed. Thus, each user identifier in the user table comprises a user symbol and the user's decrypting sender public key, wherein the user authentication message comprises an encrypted user authentication message which may be decrypted by the user decrypting key, specifically comprising a request for access encrypted by a sender private key and a receiver public key, and wherein the employed private key, public key cryptographic algorithm decrypts the user authentication message employing a receiver private key and the sender public key, whereby the user authentication message is known to have come from the user.

The permitted activities in the user table may comprise 1) read access to data stored in the data storage media, 2) write access to data stored in the data storage media, 3) read the user entry of the user table, 4) read all entries of the user table, 5) add entries to the user table, and 6) change/delete entries to the user table. Each of the users may be authorized to conduct selected ones of the plurality of activities.

A class table is additionally provided that has an unique class identifier for each authorized class of users, which may comprise a class symbol and a corresponding class key and at least one permitted activity each class of users is authorized to conduct with respect to the data storage media. The class identifier, when combined with a user authentication message from a user of the authorized class of users in accordance with the predetermined algorithm, authorizes the user. The user table additionally comprises any class membership of each user, wherein the user may be authorized with respect to the class table either by the class authorization or by the user authorization. The user table permitted activities may additionally comprise 3) read all entries of the class table, 4) add entries to the class table, and 5) change/delete entries to the class table.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will now be described in more detail, by way of example, with reference to the accompanying drawings in which:

FIG. 1 is a diagrammatic representation of a data storage cartridge with a data storage drive and a host in accordance with the present invention;

FIG. 2 is a block diagram of an RF interface, computer processor, and nonvolatile storage in the data storage cartridge of FIG. 1;

FIGS. 3 and 4 are diagrammatic representations of tables of the nonvolatile storage of FIG. 2;

FIG. 5 is a diagrammatic representation of the encryption of a request for access and its decryption in accordance with the present invention;

FIG. 6 is a diagrammatic representation of a state diagram of the operation of the computer processor of FIG. 2 in accordance with the present invention; and

FIGS. 7 and 8 are flow charts depicting the method of the present invention for initializing a data storage cartridge and for conducting the authentication and authorization of a user request.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

This invention is described in preferred embodiments in the following description with reference to the Figures, in which like numbers represent the same or similar elements. While this invention is described in terms of the best mode for achieving this invention's objectives, it will be appreciated by those skilled in the art that variations may be accomplished in view of these teachings without deviating from the spirit or scope of the invention.

Referring to FIG. 1, a data storage cartridge 10, such as a magnetic tape cartridge (as illustrated) or an optical disk, is loaded into a data storage drive 11. An example of a data storage cartridge is an IBM 3590

data tape cartridge. Another example is an LTO (Linear Tape Open) data tape cartridge.

The data storage cartridge has a storage media 12, such as a magnetic tape, that is stored on a tape reel 15 and may be threaded into the data storage drive 11. As an example, the magnetic tape 12 is threaded past a read/write head 17 to a take-up reel 18. A drive controller 20, which includes both read/write electronics and control circuitry for operating the drive, is coupled to the read/write head 17 for reading data from, or writing data to, the storage media 12. The drive controller is also coupled, via an interface 21, to a host 22. The host may comprise a data processing system or server, or may comprise a drive subsystem controller, for example, for an automated data storage library. An example of a data storage drive is an IBM 3590 tape storage subsystem.

The data storage drive 11 is modified so that drive controller 20 is also coupled to a wireless interface 25. The data storage cartridge 10 is also modified to incorporate a wireless interface 26 and a computer processor 30 with a nonvolatile memory 31.

The cartridge wireless interface 26 receives power and data from, and sends data to, the wireless interface 25 of the data storage drive when the data storage cartridge 10 is mounted in the data storage drive 11. Preferably, the wireless interface 25, 26 is an RF wireless interface. An example is described in U.S. Patent No. 4,941,201. A high frequency inductive wireless interface may also be employed, which is of sufficiently high frequency that the magnetic storage media 12 is not adversely affected by the signal. Examples are described in U.S. Patents No. 4,650,981, No. 4,758,836, and No. 3,859,624. Alternatively, the inductive antennae for the wireless interface are shielded from the magnetic storage media 12.

The computer processor 30 comprises a microprocessor chip, for example, an Intel Pentium chip arranged to operate in a low power environment, such as a portable computer, and the associated nonvolatile memory 31 is also arranged to operate in a low power environment.

In accordance with the present invention, the wireless interface 26 and the computer processor 30 with the associated nonvolatile memory 31

are mounted in, and provide a portable security system for, the portable data storage cartridge 10. Specifically, the security system, by being mounted in the portable data storage cartridge, becomes portable, accompanying the cartridge at all times. Thus, the security is no longer exclusively dependent upon the security of the data storage drive 11 and its host system 22, and is not limited to a particular drive or host. The cartridge may be used with different drives and host systems at varied locations, and may be used with updated drives and updated data processing systems. Further, the security system may be managed and updated to change access to the data at any of the drives by users which have previously been granted permission via the user or class tables in the data storage cartridge. The security system remains portable and within the data storage cartridge.

The wireless interface 26 and computer processor 30 are detailed in FIG. 2. An antenna 35 receives the RF signal from the RF interface of the data storage drive, and coupler 36 supplies the received signal to a power conversion circuit 40, and to a data demodulator 42. The power conversion circuit 40 converts the received signal to a power current, supplying the current on line 44 to all of the devices in the data storage cartridge requiring power, including the computer processor 30, the data demodulator 42, and a data modulator 45. The received signal from antenna 35 is encoded, and data demodulator 42 receives the incoming coded signal from coupler 36 and demodulates the signal to provide data signals to the computer processor 30. Data signals from the computer processor 30 are provided to the data modulator 45 which encodes the signals for transmission by coupler 36 and antenna 35 to the RF interface of the data storage drive.

The computer processor 30 is a programmable computer processor comprising a microprocessor 37 having computer readable program code embodied therein, including an encryption/decryption algorithm 38 and an authorization/authentication/permitted activities algorithm 39. The nonvolatile storage 31 is employed to store user and class tables, as will be explained. The nonvolatile storage may comprise a separate chip attached to the programmable computer processor 30 and its microprocessor 37, or may comprise a portion of the same chip. The computer readable program code may be stored in a nonvolatile internal memory of the computer processor 30 or may also be stored in the nonvolatile memory 31, and loaded into the computer processor 30. The algorithms 38 and 39 may

be preloaded into the programmable computer processor **30**, or may be supplied to the computer processor at initialization over the wireless interface **26**.

The computer processor **30**, employing the algorithm **39**, provides a user table in nonvolatile memory **31** comprising at least a unique user identifier for each authorized user, which may comprise a user symbol and a corresponding key, and at least one permitted activity the user is authorized to conduct with respect to the data storage media, and provides a class table in nonvolatile memory **31** which has unique class identifier for each authorized class of users, which may comprise a class symbol and a corresponding key, and at least one permitted activity each class of users is authorized to conduct with respect to the data storage media.

In accordance with the predetermined algorithm **39**, the user identifier, when combined with a user authentication message from the authorized user, employing the encryption/decryption algorithm **38**, authorizes the user. The computer processor **30** receives user authentication messages from the data storage drive via the wireless interface **26**, and combines the user authentication message with the user identifier from the user table in accordance with the predetermined algorithm **39** and encryption/decryption algorithm **38** to authorize or deny the user activity, and transmits the user authorization or denial to the data storage drive via the wireless interface **26**.

Herein, the encryption/decryption algorithm **38** comprises any suitable encryption/decryption algorithm which both provides security and portability. Examples of algorithms which provide security and portability are the "public key" cryptography algorithms. U.S. Patent No. 4,405,829 describes a "public key" encryption/decryption algorithm that has become a defacto-standard, often called the "RSA" cryptosystem after the names of the authors. An implementation that provides authentication and allows authorization as employed herein is described in U.S. Patent No. 4,748,668. Accordingly, the user identifier comprises a user symbol and a user decrypting sender public key. When combined with a user authentication message from the authorized user that is encrypted by a receiver public key, the user is authorized. Additionally, with the use of a sender private key and the receiver public key, the authentication message can be encrypted so that, with the use of a receiver private key

and the sender public key, the authentication message is both decrypted and the message is known to have come from the sender.

FIGS. 3, 4 and 5 illustrate examples of cartridge initialization with the user and class tables and the operation of the algorithm 39 employing the cryptography algorithm 38. FIG. 3 illustrates an uninitialized data storage cartridge 10 either without user and class tables, or which has established user and class tables, but which are empty. FIG. 4 illustrates the data storage cartridge 10 after the user table 50 and the class table 51 have been initialized in accordance with the present invention.

As discussed above, the computer processor 30 provides the user table 50 with at least a unique user identifier for each authorized user and at least one permitted activity the user is authorized to conduct with respect to the data storage media. Preferably, each user identifier in the user table 50 comprises a user symbol 54 and a user decrypting sender public key 55. The permitted activities 56 of the user may comprise a separate entry for each user identifier and permitted activity that the user is authorized to conduct. Alternatively, the user table may comprise a separate entry for each user identifier, the entry comprising all of the permitted activities that the user is authorized to conduct. The user table 50 additionally comprises any class membership 57 of each user, so that the user may be authorized with respect to the class table 51 by the user authorization.

In accordance with the present invention, the class table 51 is provided that has an unique class identifier for each authorized class of users, and at least one permitted activity 64 that each class of users is authorized to conduct. Preferably each class identifier in the class table 51 comprises a class symbol 62 and a class decrypting sender public key 63. The class identifier, when combined with a user authentication message from a user of the authorized class of users in accordance with the predetermined algorithm, authorizes the user. Thus, the user may be authorized with respect to the class table either by the class authorization or by the user authorization 57.

The permitted activities 64 of the members of the class may comprise a separate entry for each class identifier and permitted activity that the user/class member is authorized to conduct. Alternatively, the class

table may comprise a separate entry for each class identifier, the entry comprising all of the permitted activities that the user/class member is authorized to conduct.

The permitted activities **56** in the user table **50** may comprise 1) read access to data stored in the data storage media, 2) write access to data stored in the data storage media, 3) read user entry of the user table, 4) read all entries of the user table, 5) add entries to the user table, 6) change/delete entries to the user table, 7) read class entry of the class table, 8) read all entries of the class table, 9) add entries to the class table, 10) change/delete entries to the class table, and 11) change the receiver private key.

The permitted activities **64** in the class table **51** may comprise 1) read access to data stored in the data storage media, 2) write access to data stored in the data storage media, 3) read the user's class entry of the class table, 4) read all entries of the class table, 5) add entry to the class table, 6) change/delete entries to the class table, 7) read all entries of the user table, 8) add entries to the user table, 9) change/delete entries to the user table and 10) change the receiver private key.

The operation of a public key algorithm for authorizing access is illustrated with respect to FIG. **5**. The preferred implementation is one as described above which both allows an authentication message to be decrypted, and also provides a "signature" assuring that the authentication message has come from the sender. In one example, the user/class symbol will have been sent. A user/class member generates an authentication message **70**. Preferably, the authentication message includes the request for access to conduct the desired activity, saving a need for a second message. The user/class member has a sender private key **71** which is employed, together with a receiver public key **72**, to encrypt the authentication message. The receiver public key **72** is made known to the users and class members and is mathematically related to the sender private key, as discussed in the '668 patent, but the message cannot be decrypted with the same keys. The message instead is only readable by the intended receiver because of the use of the receiver public key. When decrypted, the message must have therefore been intended for the receiver. Thus, at the cartridge, the algorithm of the computer processor decrypts the message employing a receiver private key **73** and a sender public key

74. As discussed above, the sender public key has been made available and is kept in the user table or in the class table. Thus, if the keys decrypt the encrypted authentication message, the message is known to have come from the sender who is the user/class member. This is known as providing an authentication "signature".

As the result, the user/class member may rely on the security of the portable security system, method, and computer readable program code of a computer program product, of the present invention, which resides in a portable data storage cartridge for managing access to the portable data storage cartridge.

A state diagram of the operation of the computer processor in accordance with the present invention is illustrated in FIG. 6, and flow charts of the method of the present invention are depicted in FIGS. 7 and 8.

Referring to FIGS. 1 and 7, the initialization of an uninitialized cartridge 10 is initiated at step 80. The cartridge is loaded into a drive 11 having a wireless interface 25, and, in step 81, the initialization information is transmitted to the cartridge. The initialization information is not encrypted, and is provided when in a secure situation. The cartridge wireless interface 26 receives the initialization information in step 82 and provides the information to the cartridge processor 30. As discussed above, the initialization information comprises the user and class tables. The cartridge processor 30, in step 83, recognizes that the input from the wireless interface is initialization information, and determines whether the cartridge is uninitialized. If the cartridge has been initialized previously, a message is sent to the drive 11 over the wireless interface, in step 84, denying the initialization.

If the cartridge is uninitialized, an initializing drive or host computer provides the user table to the cartridge computer processor 30 in step 85 and provides the class table in step 86, both via the wireless interface. The receiver private key may have been provided previously, or, as an optional step 87, may be provided in the initialization load. The initialization is then complete, and the drive is informed of the completion in step 89.

Referring to FIGS. 1, 6 and 8, an authentication or an access request is initiated in step 90, e.g., by sending the user symbol, and the cartridge computer processor 30 is initially in an idle state 91. In step 93, the request is received at the wireless interface 26 and is provided to the computer processor. The computer processor moves to state 94 and, in step 95, determines whether the requesting user or class member is in the list of the user or class table. If not in the table, the computer processor 30, in step 96, moves to state 97 and denies access to the user/class member via the wireless interface 26.

If the user or class member is in the respective table, the computer processor, in step 98, moves to state 99 and requests the authentication message from the user or class member. The computer processor moves to state 100 while awaiting the authentication message, and, if the message is not received in a time out period, denies access in state 97. In step 102, the authentication message is received by the wireless interface 26 and forwarded to the computer processor 30. As discussed above, the authentication message is encrypted by the sender private key and the receiver (cartridge) public key. The computer processor moves to state 103, receiving the message and beginning the authentication. In step 105, the computer processor conducts the decryption of the authentication message employing the receiver private key and employing the sender public key from the user or class table. In step 106, the computer processor determines whether the user or class member is authorized. If not, the computer processor 30 moves to state 97 and, in step 96, denies access.

If the user or class member is authorized, the computer processor moves to state 98 and, in step 110, reads the user or class table for the permitted activities for the user/class member. As discussed above, the authentication message preferably includes a request to conduct one or more activities. Based on the permitted activities of the user or class table and the request, the computer processor moves to state 111 or to state 112 to grant the permitted activity. The permission to change the receiver private key will be very limited to a particular user or to a particular class. Thus, the grant of the permitted activities of state 111 are transmitted in step 114 to the drive 11 over the wireless interface. As an example, the requested access from state 111 does not require a decrypting key for the data, such as changing an entry to the user table. State 112 is entered only in response to a specific request by the user/class member, and, in step 114, the decrypting key for the

data on the cartridge data storage media is transmitted to the drive 11 from the cartridge 10 over the wireless interface 26. The computer processor then moves back to the idle state 91, and the data may be read.

As specific security examples, read access to the data stored in the data storage media is controlled by the computer processor 30 in the portable cartridge through the decrypting key; table access is enforced by the computer processor 30 in the portable cartridge; and write access is controlled logically in the drive, which may be under the logical control of the processor. However, the cartridge itself cannot totally restrict writing per se.

Thus, the present invention provides a security system which is portable and may be managed to accommodate changes to access to the data of the data storage cartridge 10. Only certain users are allowed access to each cartridge, and only certain users are allowed to define who has access to that data.

CLAIMS

1. A portable security system for managing access to a portable data storage cartridge, said data storage cartridge having data storage media for storing data for read/write access by a user of a data storage drive when mounted in said data storage drive, said portable security system comprising:

a wireless interface mounted in said portable data storage cartridge for receiving power and data from, and sending data to, said data storage drive when mounted in said data storage drive; and

a computer processor mounted in said portable data storage cartridge and coupled to said wireless interface; said computer processor powered by said wireless interface and receiving and transmitting data to said data storage drive via said wireless interface; said computer processor having a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media, said user identifier, when combined with a user authentication message from said authorized user in accordance with a predetermined algorithm, authorizes said user; said computer processor receiving said user authentication messages from said data storage drive via said wireless interface, combining said user authentication message with said user identifier from said user table in accordance with said predetermined algorithm to authorize or deny said user activity, and transmitting said user authorization or denial to said data storage drive via said wireless interface.

2. The portable security system of Claim 1, wherein said wireless interface comprises an RF interface.

3. The portable security system of Claim 1 or claim 2, wherein each said user identifier comprises a user symbol and a user decrypting key, wherein said user authentication message comprises an encrypted user authentication message which may be decrypted by said user decrypting key, and wherein said computer processor conducts said combination by decrypting said user authentication message by said user decrypting key.

4. The portable security system of Claim 3, wherein said user decrypting key comprises a sender public key, and wherein said predetermined algorithm comprises a public key cryptographic algorithm.

5. The portable security system of Claim 4, wherein said user authentication message is encrypted by a sender private key and a receiver public key, and wherein said public key cryptographic algorithm decrypts said user authentication message employing a receiver private key and said sender public key, whereby said user authentication message is known to have come from said user.

6. The portable security system of any one of the preceding claims, wherein said computer processor user table permitted activities comprise a plurality of permitted activities, selected ones of which each of said users may be authorized to conduct, said permitted activities comprising 1) read access to data stored in said data storage media, 2) write access to data stored in said data storage media, 3) read the user entry of said user table, 4) read all entries of said user table, 5) add entries to said user table, and 6) change/delete entries to said user table.

7. The portable security system of any one of the preceding claims, wherein said computer processor user table comprises a separate entry for each said user identifier and said permitted activity said user is authorized to conduct.

8. The portable security system of any one of claims 1 to 6, wherein said computer processor user table comprises a separate entry for each said user identifier, said entry comprising all said permitted activities said user is authorized to conduct.

9. The portable security system of any one of the preceding claims, wherein said computer processor additionally comprises a nonvolatile memory storing said user table.

10. The portable security system of any one of the preceding claims, wherein said computer processor additionally comprises a class table comprising at least a unique class identifier for each authorized class of users and at least one permitted activity said class of users is authorized to conduct with respect to said data storage media, said class identifier, when combined with a user authentication message from a user of said authorized class of users in accordance with said predetermined algorithm, authorizes said user; and wherein said computer processor additionally, upon receiving said user authentication messages from said data storage drive via said wireless interface, combining said user

authentication message with said class identifier from said class table in accordance with said predetermined algorithm to authorize or deny said class activity to said user, and transmitting said class authorization or denial to said data storage drive via said wireless interface.

11. The portable security system of Claim 10, wherein said computer processor user table additionally comprises any class membership of each said user, wherein said user may be authorized with respect to said class table either by said class authorization or by said user authorization.

12. The portable security system of Claim 10 or Claim 11, wherein said computer processor user table and said class table permitted activities comprise a plurality of permitted activities, selected ones of which each of said users may be authorized to conduct, said permitted activities comprising 1) read access to data stored in said data storage media, 2) write access to data stored in said data storage media, 3) read all entries of said class table, 4) add entries to said class table, and 5) change/delete entries to said class table.

13. The portable security system of any preceding claim, wherein said data stored in said data storage media is encrypted, wherein said computer processor user table permitted activities comprise at least 1) read access to data stored in said data storage media, and wherein said user authorization for said read access additionally comprises a decryption key for said encrypted stored data.

14. A data storage cartridge for storing data for read/write access by a user of a data storage drive when mounted in said data storage drive, comprising:

data storage media mounted in said data storage cartridge for storing said data for said read/write access;

a wireless interface mounted in said portable data storage cartridge for receiving power and data from, and sending data to, said data storage drive when mounted in said data storage drive; and

a computer processor mounted in said portable data storage cartridge and coupled to said wireless interface; said computer processor powered by said wireless interface and receiving and transmitting data to said data storage drive via said wireless interface; said computer processor having a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity said user is

authorized to conduct with respect to said data storage media, said user identifier, when combined with a user authentication message from said authorized user in accordance with a predetermined algorithm, authorizes said user; said computer processor receiving said user authentication messages from said data storage drive via said wireless interface, combining said user authentication message with said user identifier from said user table in accordance with said predetermined algorithm to authorize or deny said user activity, and transmitting said user authorization or denial to said data storage drive via said wireless interface.

15. The data storage cartridge of Claim 14, wherein said wireless interface comprises an RF interface.

16. The data storage cartridge of Claim 14 or Claim 15, wherein each said user identifier comprises a user symbol and a user decrypting key, wherein said user authentication message comprises an encrypted user authentication message which may be decrypted by said user decrypting key, and wherein said computer processor conducts said combination by decrypting said user authentication message by said user decrypting key.

17. The data storage cartridge of Claim 16, wherein said user decrypting key comprises a sender public key, and wherein said predetermined algorithm comprises a public key cryptographic algorithm.

18. The data storage cartridge of Claim 17, wherein said user authentication message is encrypted by a sender private key and a receiver public key, and wherein said public key cryptographic algorithm decrypts said user authentication message employing a receiver private key and said sender public key, whereby said user authentication message is known to have come from said user.

19. The data storage cartridge of any one of claims 14 to 18, wherein said computer processor user table permitted activities comprise a plurality of permitted activities, selected ones of which each of said users may be authorized to conduct, said permitted activities comprising 1) read access to data stored in said data storage media, 2) write access to data stored in said data storage media, 3) read the user entry of said user table, 4) read all entries of said user table, 5) add entries to said user table, and 6) change/delete entries to said user table.

20. The data storage cartridge of any one of claims 14 to 19, wherein said computer processor user table comprises a separate entry for each said user identifier and said permitted activity said user is authorized to conduct.

21. The data storage cartridge of any one of claims 14 to 19, wherein said computer processor user table comprises a separate entry for each said user identifier, said entry comprising all said permitted activities said user is authorized to conduct.

22. The data storage cartridge of any one of claims 14 to 21, wherein said computer processor additionally comprises a nonvolatile memory storing said user table.

23. The data storage cartridge of any one of claims 14 to 22, wherein said computer processor additionally comprises a class table comprising at least a unique class identifier for each authorized class of users and at least one permitted activity said class of users is authorized to conduct with respect to said data storage media, said class identifier, when combined with a user authentication message from a user of said authorized class of users in accordance with said predetermined algorithm, authorizes said user; and wherein said computer processor additionally, upon receiving said user authentication messages from said data storage drive via said wireless interface, combining said user authentication message with said class identifier from said class table in accordance with said predetermined algorithm to authorize or deny said class activity to said user, and transmitting said class authorization or denial to said data storage drive via said wireless interface.

24. The data storage cartridge of Claim 23, wherein said computer processor user table additionally comprises any class membership of each said user, wherein said user may be authorized with respect to said class table either by said class authorization or by said user authorization.

25. The data storage cartridge of Claim 23 or Claim 24, wherein said computer processor user table and said class table permitted activities comprise a plurality of permitted activities, selected ones of which each of said users may be authorized to conduct, said permitted activities comprising 1) read access to data stored in said data storage media, 2) write access to data stored in said data storage media, 3) read all

entries of said class table, 4) add entries to said class table, and 5) change/delete entries to said class table.

26. The data storage cartridge of any one of claims 14 to 25, wherein said data stored in said data storage media is encrypted, wherein said computer processor user table permitted activities comprise at least 1) read access to data stored in said data storage media, and wherein said user authorization for said read access additionally comprises a decryption key for said encrypted stored data.

27. A method for providing a portable secure interface to a data storage cartridge, said data storage cartridge having data storage media for storing data for read/write access by a user of a data storage drive when mounted in said data storage drive, and a wireless interface mounted in said portable data storage cartridge for receiving power and data from, and sending data to, said data storage drive when mounted in said data storage drive, said data storage cartridge having a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media, said user identifier, when combined with a user authentication message from said authorized user in accordance with a predetermined algorithm, authorizes said user, said method comprising the steps of:

receiving said user authentication messages from said data storage drive via said wireless interface;

combining said user authentication message with said user identifier from said user table in accordance with said predetermined algorithm to authorize or deny said user activity; and

transmitting said user authorization or denial to said data storage drive via said wireless interface.

28. The method of Claim 27, wherein each said user identifier comprises a user symbol and a user decrypting key, wherein said user authentication message comprises an encrypted user authentication message which may be decrypted by said user decrypting key, and wherein said combining step comprises decrypting said user authentication message by said user decrypting key.

29. The method of Claim 27 or Claim 28, wherein said user decrypting key comprises a sender public key, and wherein said predetermined algorithm comprises a public key cryptographic algorithm.

30. The method of Claim 29, wherein said user authentication message is encrypted by a sender private key and a receiver public key, wherein said public key cryptographic algorithm decrypts said user authentication message employing a receiver private key and said sender public key, and wherein said combining step comprises decrypting said user authentication message by said receiver private key and said sender public key, whereby said user authentication message is known to have come from said user.

31. The method of any one of claims 27 to 30, wherein said user table comprises a plurality of said permitted activities, selected ones of which each of said users may be authorized to conduct, said permitted activities comprising 1) read access to data stored in said data storage media, 2) write access to data stored in said data storage media, 3) read the user entry of said user table, 4) read all entries of said user table, 5) add entries to said user table, and 6) change/delete entries to said user table; and wherein said transmitting step comprises transmitting authorization to conduct the selected said user permitted activities said user is authorized to conduct.

32. The method of any one of claims 27 to 31, wherein said user table comprises a separate entry for each said user identifier and said permitted activity said user is authorized to conduct; and wherein said transmitting step additionally comprises identifying said user permitted activities from said separate entries.

33. The method of any one of claims 27 to 31, wherein said step of providing said user table comprises a separate entry for each said user identifier, said entry comprising all said permitted activities said user is authorized to conduct; and wherein said transmitting step additionally comprises identifying said user permitted activities from said user separate entry.

34. The method of any one of claims 27 to 33, wherein said data storage cartridge additionally comprises a class table comprising at least a unique class identifier for each authorized class of users and at least one permitted activity said class of users is authorized to conduct with

respect to said data storage media, said class identifier, when combined with a user authentication message from a user of said authorized class of users in accordance with said predetermined algorithm, authorizes said user;

wherein said combining step additionally comprises, upon receiving said user authentication messages from said data storage drive via said wireless interface, combining said user authentication message with said class identifier from said class table in accordance with said predetermined algorithm to authorize or deny said class activity to said user; and

wherein said transmitting step additionally comprises transmitting said class authorization or denial to said data storage drive via said wireless interface.

35. The method of Claim 34, wherein said user table additionally comprises any class membership of each said user; and wherein said combining step additionally authorizes said user with respect to said class table either by said class authorization or by said user authorization.

36. The method of Claim 34 or Claim 35, wherein said user table and said class table comprise a plurality of permitted activities, selected ones of which each of said users may be authorized to conduct, said permitted activities comprising 1) read access to data stored in said data storage media, 2) write access to data stored in said data storage media, 3) read all entries of said class table, 4) add entries to said class table, and 5) change/delete entries to said class table; and wherein said transmitting step comprises transmitting authorization to conduct the selected said user and said class permitted activities said user is authorized to conduct.

37. The method of any of claims 27 to 36, wherein said data stored in said data storage media is encrypted, wherein said step of providing said user table permitted activities comprises providing at least 1) read access to data stored in said data storage media, and wherein said step of transmitting said user authorization for said read access additionally comprises transmitting a decryption key for said encrypted stored data.

38. A computer program product usable with a programmable computer processor having computer readable program code embodied therein for providing a secure interface to a data storage cartridge, said programmable computer processor mounted in said data storage cartridge, said data storage cartridge having data storage media for storing data for read/write access by a user of a data storage drive when mounted in said data storage drive, and a wireless interface mounted in said portable data storage cartridge for receiving power and data from, and sending data to, said data storage drive when mounted in said data storage drive, said computer program product comprising:

computer readable program code which causes said programmable computer processor to provide a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media, said user identifier, when combined with a user authentication message from said authorized user in accordance with a predetermined algorithm, authorizes said user;

computer readable program code which causes said programmable computer processor to receive said user authentication messages from said data storage drive via said wireless interface;

computer readable program code which causes said programmable computer processor to combine said user authentication message with said user identifier from said user table in accordance with said predetermined algorithm to authorize or deny said user activity; and

computer readable program code which causes said programmable computer processor to transmit said user authorization or denial to said data storage drive via said wireless interface.

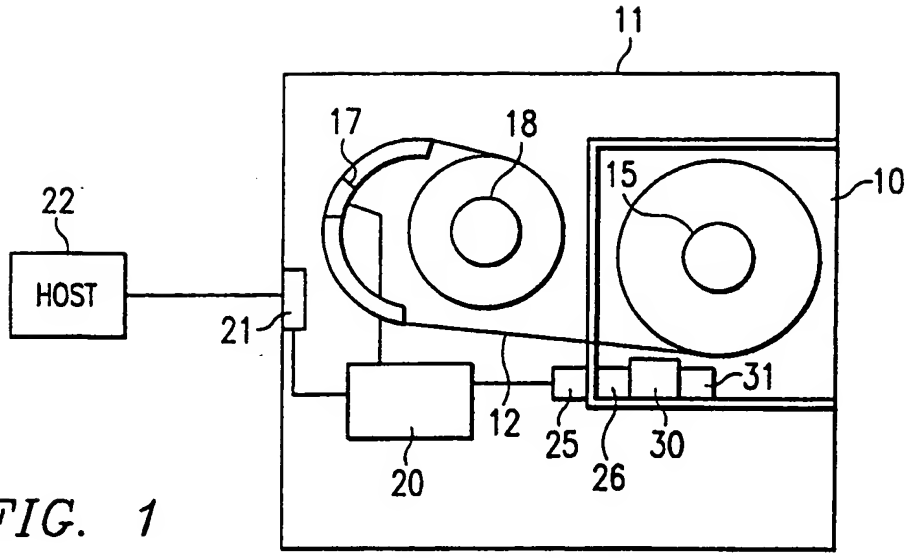

11
17
18
15
10
22
HOST
21
31
12
25
26
30
20

FIG. 1

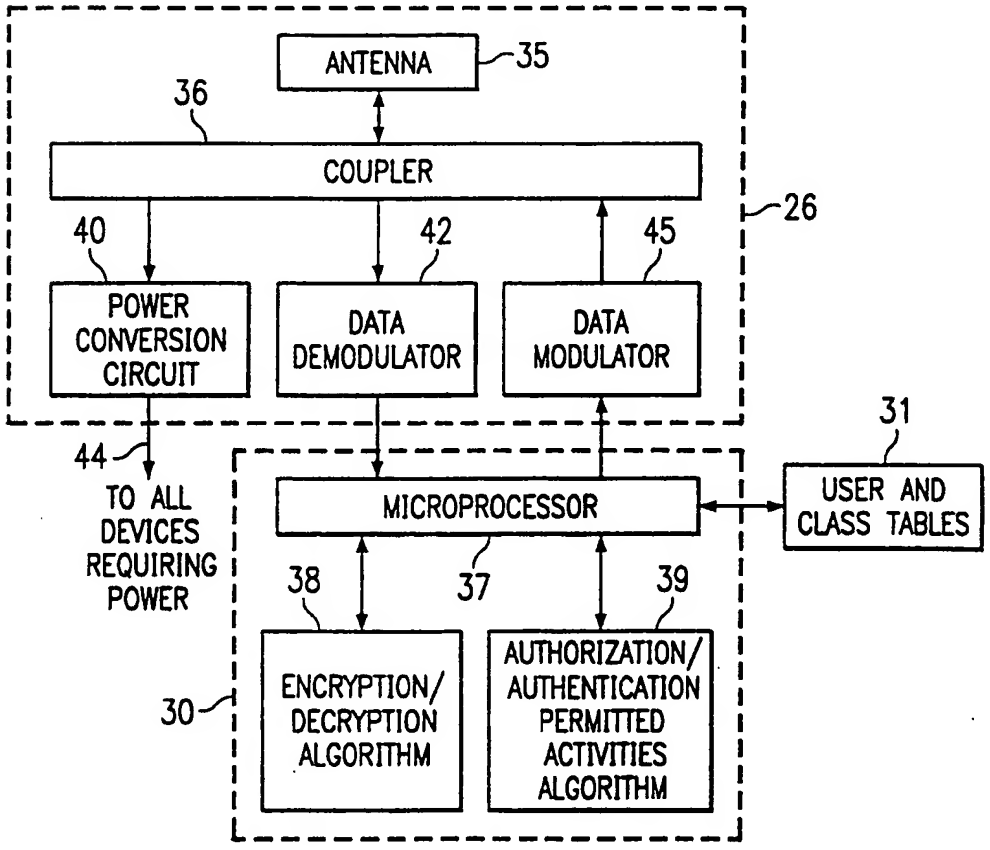

ANTENNA
35
36
COUPLER
26
40
42
45
POWER CONVERSION CIRCUIT
DATA DEMODULATOR
DATA MODULATOR
31
44
TO ALL DEVICES REQUIRING POWER
MICROPROCESSOR
USER AND CLASS TABLES
38
37
39
30
ENCRYPTION/ DECRYPTION ALGORITHM
AUTHORIZATION/ AUTHENTICATION PERMITTED ACTIVITIES ALGORITHM

FIG. 2

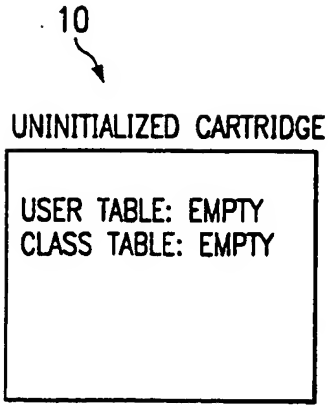


FIG. 3

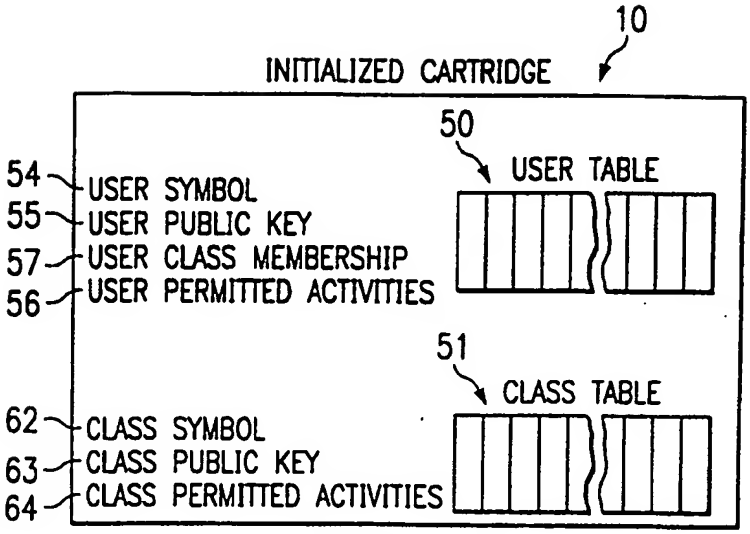


FIG. 4

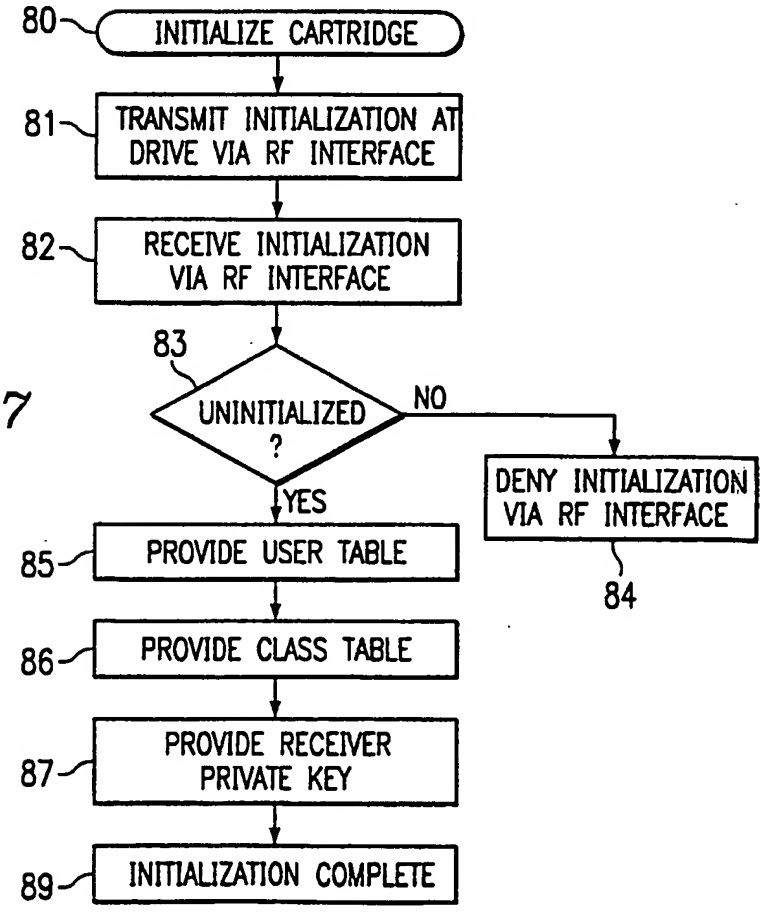


FIG. 7

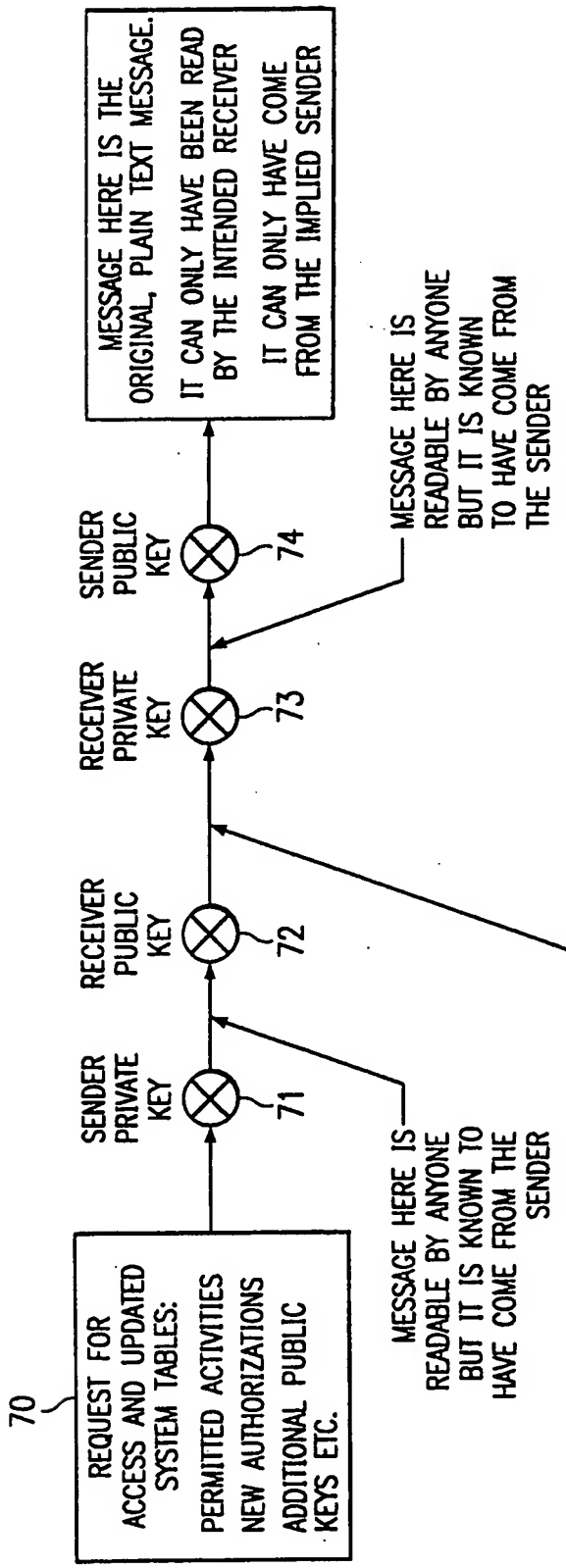

70
REQUEST FOR ACCESS AND UPDATED SYSTEM TABLES:
PERMITTED ACTIVITIES
NEW AUTHORIZATIONS
ADDITIONAL PUBLIC KEYS ETC.
SENDER PRIVATE KEY
71
RECEIVER PUBLIC KEY
72
RECEIVER PRIVATE KEY
73
SENDER PUBLIC KEY
74
MESSAGE HERE IS THE ORIGINAL, PLAIN TEXT MESSAGE.
IT CAN ONLY HAVE BEEN READ BY THE INTENDED RECEIVER
IT CAN ONLY HAVE COME FROM THE IMPLIED SENDER
MESSAGE HERE IS READABLE BY ANYONE BUT IT IS KNOWN TO HAVE COME FROM THE SENDER
MESSAGE HERE IS READABLE BY ANYONE BUT IT IS KNOWN TO HAVE COME FROM THE SENDER
MESSAGE HERE IS READABLE ONLY BY THE INTENDED RECEIVER

FIG. 5

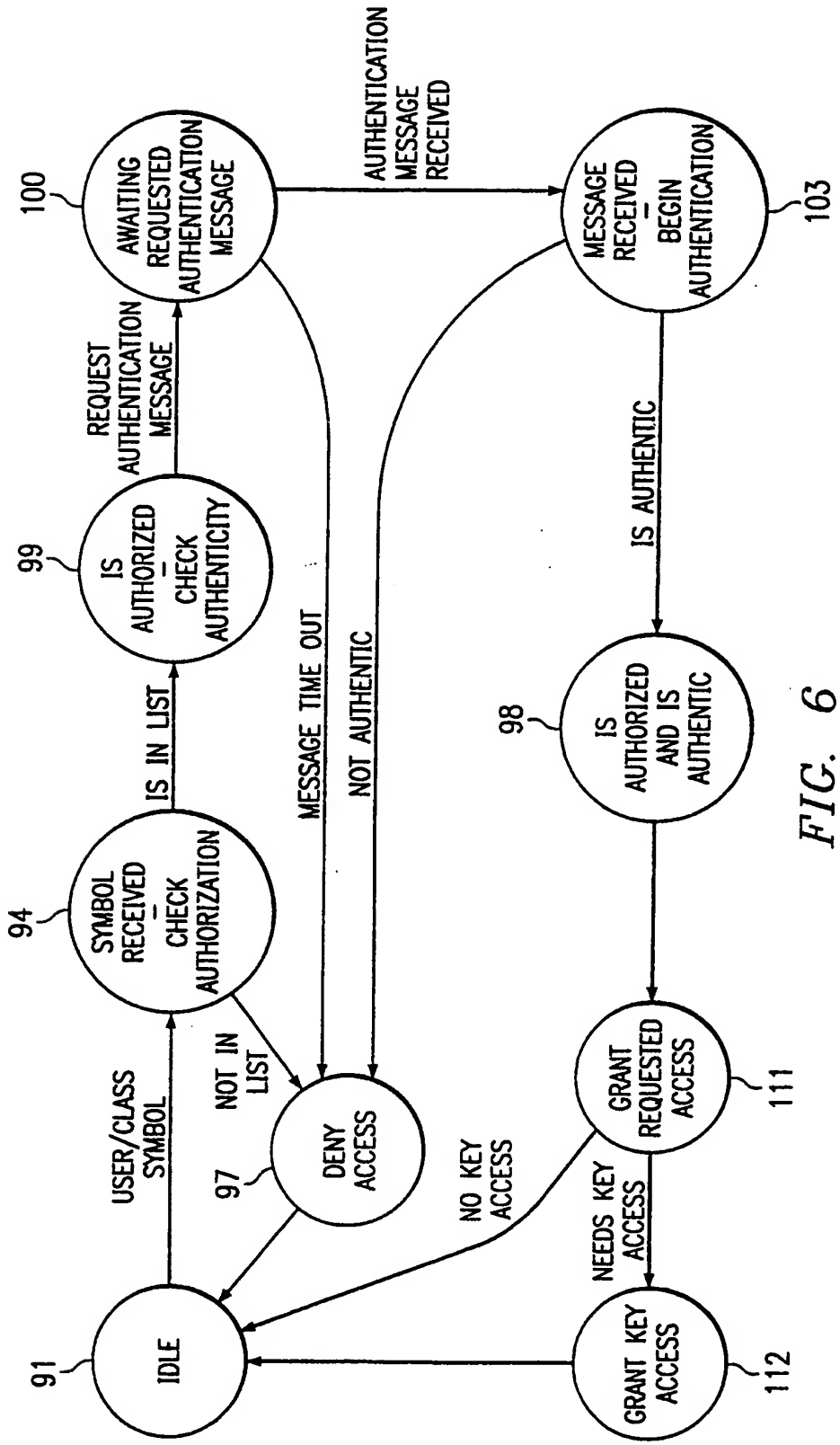

91
IDLE
USER/CLASS SYMBOL
94
SYMBOL RECEIVED – CHECK AUTHORIZATION
IS IN LIST
99
IS AUTHORIZED – CHECK AUTHENTICITY
REQUEST AUTHENTICATION MESSAGE
100
AWAITING REQUESTED AUTHENTICATION MESSAGE
AUTHENTICATION MESSAGE RECEIVED
103
MESSAGE RECEIVED – BEGIN AUTHENTICATION
IS AUTHENTIC
98
IS AUTHORIZED AND IS AUTHENTIC
NEEDS KEY ACCESS
112
GRANT KEY ACCESS
NO KEY ACCESS
111
GRANT REQUESTED ACCESS
NOT IN LIST
97
DENY ACCESS
MESSAGE TIME OUT
NOT AUTHENTIC

FIG. 6

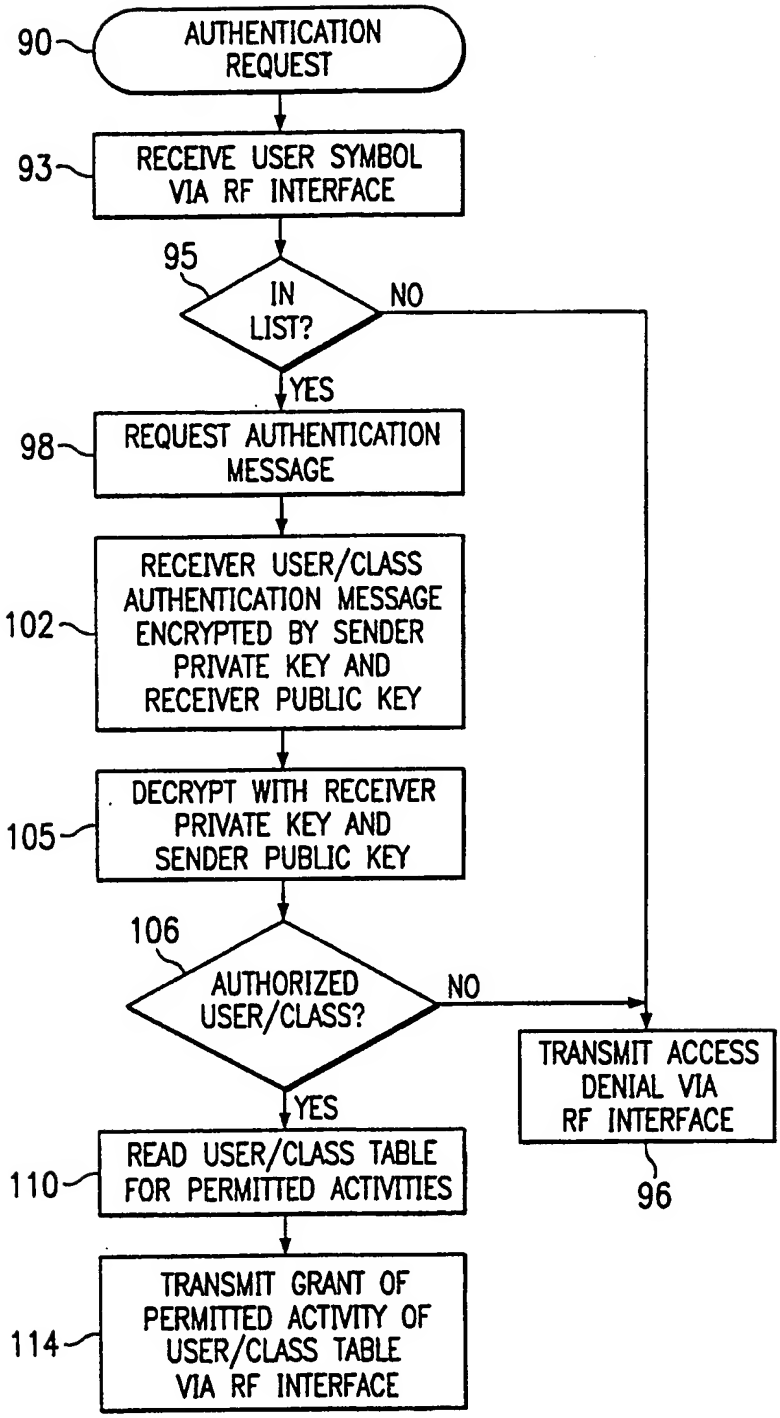

90
AUTHENTICATION REQUEST
93
RECEIVE USER SYMBOL VIA RF INTERFACE
95
IN LIST?
NO
YES
98
REQUEST AUTHENTICATION MESSAGE
102
RECEIVER USER/CLASS AUTHENTICATION MESSAGE ENCRYPTED BY SENDER PRIVATE KEY AND RECEIVER PUBLIC KEY
105
DECRYPT WITH RECEIVER PRIVATE KEY AND SENDER PUBLIC KEY
106
AUTHORIZED USER/CLASS?
NO
YES
TRANSMIT ACCESS DENIAL VIA RF INTERFACE
96
110
READ USER/CLASS TABLE FOR PERMITTED ACTIVITIES
114
TRANSMIT GRANT OF PERMITTED ACTIVITY OF USER/CLASS TABLE VIA RF INTERFACE

FIG. 8

INTERNATIONAL SEARCH REPORT

Interr nal Application No
PCT/GB 00/04266

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 857 021 A (KATAOKA SATOSHI ET AL) 5 January 1999 (1999-01-05) cited in the application abstract column 3, line 5 -column 8, line 67 ---	1,3-14, 16-38
A	WO 97 41562 A (DIEZMANN NILS ;FINKENZELLER KLAUS (DE); GIESECKE & DEVRIENT GMBH () 6 November 1997 (1997-11-06) abstract page 1 -page 5, line 19 page 15, line 5 -page 25, line 20 figures 5,6 --- -/--	1-5, 13-18, 22, 26-30, 37,38

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 January 2001	12/02/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Jacobs, P

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/GB 00/04266

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 065 429 A (LANG GERALD S) 12 November 1991 (1991-11-12) abstract column 2, line 18 -column 7, line 38 figures 1,3,4	1,3-9, 13,14, 16-22, 26-33, 37,38
A	US 5 630 057 A (HAIT JOHN N) 13 May 1997 (1997-05-13) abstract column 14, line 36 -column 18, line 11 claims 1-3 figures 1-3	1,2, 13-15, 26,27, 37,38
A	DE 196 42 575 A (NEIFER WOLFGANG) 20 May 1999 (1999-05-20)	

2

INTERNATIONAL SEARCH REPORT

...formation on patent family members

Inter ...onal Application No
PCT/GB 00/04266

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5857021 A	05-01-1999	JP 9134311 A	20-05-1997
		JP 9134330 A	20-05-1997
		EP 0773490 A	14-05-1997
WO 9741562 A	06-11-1997	DE 19616819 A	30-10-1997
		AU 2767497 A	19-11-1997
		EP 0895637 A	10-02-1999
		JP 2000509541 T	25-07-2000
		US 6044046 A	28-03-2000
US 5065429 A	12-11-1991	US 5191611 A	02-03-1993
		CA 1329657 A	17-05-1994
		EP 0465571 A	15-01-1992
		WO 9012464 A	18-10-1990
US 5630057 A	13-05-1997	CA 1340351 A	26-01-1999
		US 5581763 A	03-12-1996
		AU 3840689 A	12-01-1990
		EP 0382811 A	22-08-1990
		WO 8912864 A	28-12-1989
DE 19642575 A	20-05-1999	NONE	